(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2002 (17.01.2002)

PCT

(10) International Publication Number
WO 02/005475 A3

(51) International Patent Classification⁷: H04L 29/06

(21) International Application Number: PCT/IB01/01221

(22) International Filing Date: 9 July 2001 (09.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/614,487 11 July 2000 (11.07.2000) US

(71) Applicant *(for all designated States except US)*: **BALTIMORE TECHNOLOGIES INC.** [CA/CA]; Suite 1120, 36 Toronto Street, Toronto, Ontario M5C 2C5 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **AMDUR, Eugene** [CA/CA]; 135 George Street South #704, Toronto, Ontario M4A 4E8 (CA). **REID, Irving** [CA/CA]; 152 Saint Patrick Street, #610, Toronto, Ontario (CA). **KOCH, C., Harald** [CA/CA]; 64 Clareville Crescent, Toronto, Ontario M2J 2C1 (CA). **LAMB, Steven** [CA/CA]; 15 Ballacaine Drive, Toronto, Ontario M8Y 4A7 (CA).

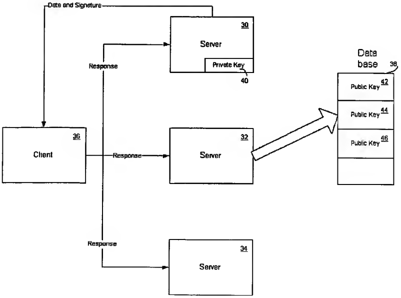
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB,*

[Continued on next page]

(54) Title: GENERATION AND USE OF DIGITAL SIGNATURES



(57) Abstract: A digital signature is generated in association with target data. The computer generating the digital data encrypts the digital signature using a public key encryption system. The private key is stored in dynamic memory in a secure manner. The public key associated with the private key is stored in an accessible database. The public key is accessed from the database and used by recipient computers to authenticate the target data by decryptiong the encrypted and used by recipient computers to authenticate the target data by decrypting the encrypted digital signature. When the computer generating the digital signature is restarted, the private key stored in dynamic memory is lost. The computer obtains a new private and public key pair from the public key encryption system. The previously used public key is maintained in the database until a predefined time has elapsed, after which it is removed from the database.

WO 02/005475 A3